RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: IAIS-T10

Building Secure AI: How Open Source, Standards and Communities Lead the Way

MODERATOR:

Scott Clinton
Co-chair, OWASP GenAI Security Project

https://www.linkedin.com/in/scottjclinton/

PANELISTS:

Arun Gupta
Chair, Linux Foundation OpenSSF, CNCF
Intel
https://www.linkedin.com/in/arunpgupta/

John Sotiropoulos
Board Member, OWASP GenAI Security Project
Kainos
https://www.linkedin.com/in/jsotiropoulos/

Omar Santos
Co-Chair, OASIS CoSAI Project
CISCO
https://www.linkedin.com/in/santosomar/

David LaBianca
Co-Chair, OASIS CoSAI Project
Google
https://www.linkedin.com/in/labianca/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices. One Community.

MODERATOR:

Scott Clinton

Co-chair, OWASP GenAI Security Project

https://www.linkedin.com/in/scottjclinton/

PANELISTS:

Arun Gupta

Chair, Linux Foundation OpenSSF & CNCF
Intel
https://www.linkedin.com/in/arunpgupta/

Omar Santos

Co-Chair, OASIS CoSAI Project
CISCO
https://www.linkedin.com/in/santosomar/

John Sotiropoulos

Board Member, OWASP GenAI Security Project
Kainos
https://www.linkedin.com/in/jsotiropoulos/

David LaBianca

Co-Chair, OASIS CoSAI Project
Google
https://www.linkedin.com/in/labianca/

OWASP GenAI SECURITY PROJECT TOP 10 FOR LLM AND GENERATIVE AI

CoSAI COALITION FOR SECURE AI

OpenSSF OPEN SOURCE SECURITY FOUNDATION

THE LINUX FOUNDATION

About - The GenAI Security Project

OWASP Foundation

- The Open Worldwide Application Security Project (OWASP) is a **nonprofit foundation that works to improve the security of software.**
- Community-led open-source projects including code, documentation, and standards
- Over **250+ local chapters** worldwide
- **200,000+** global community
- Industry-leading educational and training conferences

OWASP GenAI Security Project

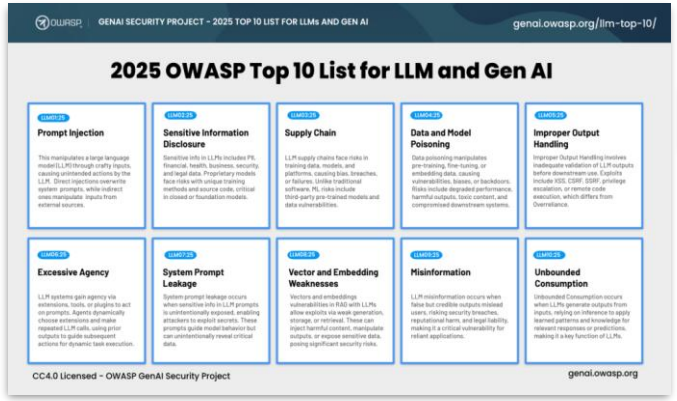
The OWASP Gen AI Security Project is a global, **open-source community project** dedicated to identifying, mitigating, and documenting security and safety risks associated with generative AI technologies, including large language models (LLMs), agentic AI systems, and AI-driven applications.

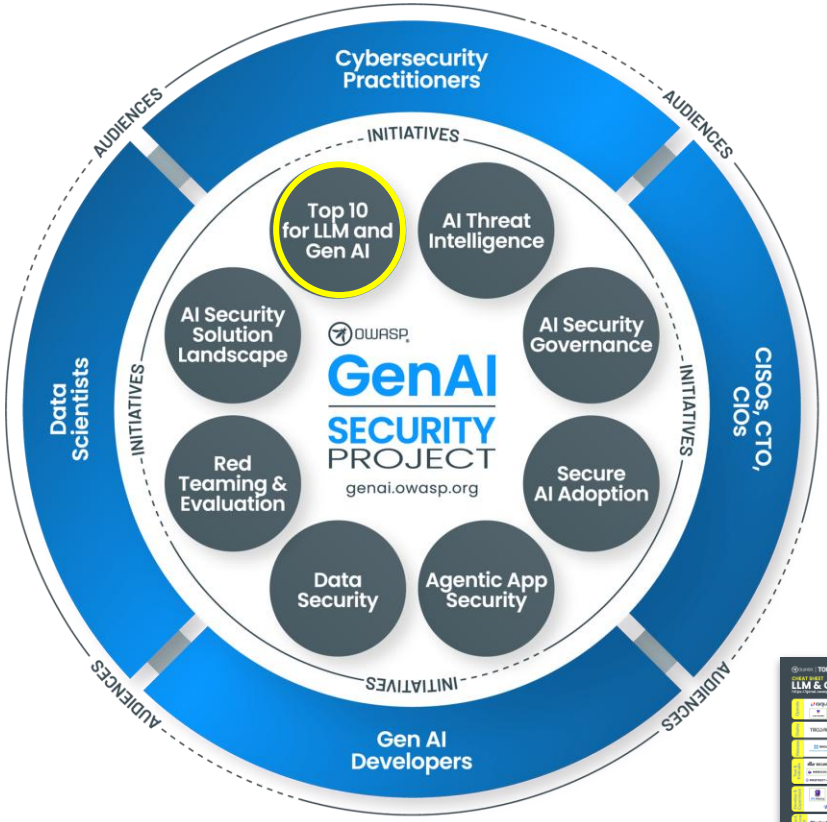
Our mission is to empower organizations, security professionals, AI practitioners, and policymakers with **comprehensive, actionable guidance and tools** to ensure the **secure development, deployment, and governance of generative AI systems**

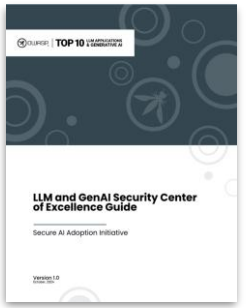
Eight Working Groups Focused On Gen AI Security Best Practices

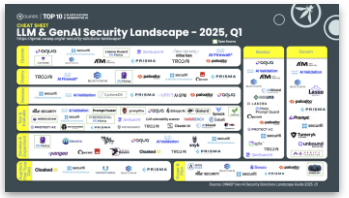
10+ expert peer reviewed resources

OWASP TOP 10 LLM APPLICATIONS & GENERATIVE AI









600+ Contributors*

130+ Supporting Companies*

2500+ Slack Members*

8000+ LI Followers*

* As of April 2025

About - OASIS CoSAI Project

- CoSAI is an open ecosystem of AI and security experts from industry-leading organizations dedicated to sharing best practices for secure AI deployment and collaborating on AI security research and product development.
- CoSAI operates under OASIS Open, the international standards and open source consortium.

CoSAI's Workstreams

CoSAI's leadership is focusing their work on these project workstreams:

Software Supply Chain Security for AI Systems

Enhance AI security by guiding the evaluation of provenance, managing third-party model risks, and assessing AI applications full provenance.
Building on SSDF and SLSA security principles, CoSAI aims to expand and refine these efforts.

Preparing Defenders for a Changing Security Landscape

Develop a defender's framework to identify investments needed to counter offensive cybersecurity capabilities of current and potential AI models.

AI Security Risk Governance

Create a risk and controls taxonomy, checklist, and scorecard to guide practitioners in readiness assessments, management, monitoring, and reporting of the security of their AI products.

Secure Design Patterns for Agentic Systems

Research and develop secure design patterns for AI-based agentic systems including updates to AI usage threat models, conceptual high-level secure design pattern(s), impacts to secure infrastructure design, and other agent integration and use based needs.

Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to sustainably secure the development, maintenance, and consumption of the open source software (OSS) we all depend on. This includes fostering collaboration, establishing best practices, and developing innovative solutions.

- **Est. 2020**
- **Security by design & Security by default**

Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. We envision a future where OSS is universally trusted, secure, and reliable. This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Copyright © 2024 The Linux Foundation®. All rights reserved. The Linux Foundation has registered trademarks and uses trademarks.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Working Groups, Projects, & SIGs

1. Inform

Vulnerability Disclosures
Efficient vulnerability reporting and remediation

V1. **CVD Guides** SIGs
V2. **Open Source Vuln Schema (OSV)** project
V3. **OpenVEX** project
- **OpenVEX** SIG

Securing Critical Projects
Identification of critical open source projects

CP1. **criticality_score** project
CP2. **Package Analysis** project

DevRel
Develop Use Cases and help others learn about security

AI/ML Security
AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

A1. **Model Signing** SIG

2. Equip

Best Practices
Identification, awareness, and education of security best practices

B1. **OpenSSF Best Practices Badge** project
B2. **OpenSSF Scorecard** project
B3. **Education** SIG
B4. **Memory Safety** SIG
B5. **C/C++ Compiler Options** SIG
B6. **Python Hardening** SIG
B7. **Security Baseline** SIG

Security Tooling
State of the art security tools

T1. **SBOM Everywhere** SIG
T2. **OSS Fuzzing** SIG
T3. **SBOMit** project
T4. **Protobom** project
T5. **bomctl** project
T6. **Fuzz Introspector** project
T7, **Minder** project

Diversity, Equity, & Inclusion
Increase representation and strengthen the overall effectiveness of the cybersecurity workforce

3. Engage

Securing Software Repositories
collaboration between repository operators

R1. **RSTUF** Project

Supply Chain Integrity
Ensuring the provenance of open source code

C1. **Security Insights** project
C2. **Supply-chain Levels for Software Artifacts (SLSA)** project
C3. **Secure Supply Chain Consumpt Framework (S2C2F)** project
C4. **gittuf** project
C5. **GUAC** project
C6. **Zarf** project

Projects
Category-leading software initiatives

P1. **Alpha Omega**
P2. **Sigstore**
P3. **Core Toolchain Infrastructure** (CTI)

GenAI Security Collaboration

Challenges

- Generative AI is advancing rapidly, outpacing traditional security approaches
- Securing these systems requires deep knowledge of both traditional and AI-specific threats
- Current security frameworks need adaptation to address generative AI's unique risks
- As generative AI is integrated into critical workflows, the potential impact of vulnerabilities grows

Disruptions

- No single security solution fits all — community input is essential
- Everyone should have access to the knowledge needed to secure AI systems
- As new AI security challenges emerge, broad community involvement is needed to create and share solutions
- We can build secure AI by extending traditional security expertise

RSAC 2025 Conference

#RSAC

Many Voices. One Community.

MODERATOR:

Scott Clinton

Co-chair, OWASP GenAI Security Project

https://www.linkedin.com/in/scottjclinton/

PANELISTS:

Arun Gupta

Chair, Linux Foundation OpenSSF & CNCF
Intel
https://www.linkedin.com/in/arunpgupta/

Omar Santos

Co-Chair, OASIS CoSAI Project
CISCO
https://www.linkedin.com/in/santosomar/

John Sotiropoulos

Board Member, OWASP GenAI Security Project
Kainos
https://www.linkedin.com/in/jsotiropoulos/

David LaBianca

Co-Chair, OASIS CoSAI Project
Google
https://www.linkedin.com/in/labianca/

OWASP GenAI SECURITY PROJECT TOP 10 FOR LLM AND GENERATIVE AI

CoSAI COALITION FOR SECURE AI

OpenSSF OPEN SOURCE SECURITY FOUNDATION

THE LINUX FOUNDATION

Getting Involved

OWASP GenAI SECURITY PROJECT

The OWASP Gen AI Security Project is and open community for collaboration.

- Join the Bi-weekly Open Meeting to Learn More
- Review the project roadmap, to see what's upcoming and where you might want to help
- Join the OWASP Slack
- Join an Initiative Working Group
- Contribute on Github

CoSAI COALITION FOR SECURE AI

Technical participation is FREE AND OPEN TO EVERYONE.

We're dedicated to fostering an inclusive and welcoming environment for every contributor.

Support CoSAI as a sponsor to ensure the project's success, funding the essential services our community depends.

coalitionforsecureai.org

join@oasis-open.org

OpenSSF OPEN SOURCE SECURITY FOUNDATION

All OpenSSF work streams are open to the public at no charge. Patches are always welcome!

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack.openss.org
- Contribute on GitHub
- Join at joinnow.openssf.org
- Email us at info@openss.org

Apply What You Have Learned Today

- **Embrace Open Source Security Initiatives**
  - Leverage resources, tools and frameworks from projects like the OWASP GenAI Security Project, OASIS CoSAI, and others to enhance AI security practices.
- **Utilize Open Resources**
  - Apply the continuum of community guidance and standards to Integrate secure AI practices into your organization by leveraging freely available resources and collaborating with the broader AI security community.
- **Adopt Open Standards, When They are Ready**
  - Implement best practices for securing AI architectures by aligning with standards set by organizations such as the Linux Foundation and OASIS CoSAI.
- **Engage with Community Roadmaps**
  - Participate in upcoming initiatives from OWASP, the Linux Foundation, and OASIS CoSAI to stay ahead of challenges and contribute to the community.
- **Stay Informed on Global AI Security Trend**
  - Stay informed on international approaches to balancing openness and security in AI development. Utilize tutorials, guidelines, and frameworks provided by open source communities to bolster your organization's AI security posture.

RSAC 2025 Conference

Many Voices. One Community.

Thank You

For More Information Visit

OWASP GenAI Security Project – https://genai.owasp.org

OASIS CoSAI Project – https://www.coalitionforsecureai.org/

#RSAC

Join the OWASP Gen AI Security Project at RSAC™ 2025 - Wednesday 4/30

8:30a-12:30pm

Gen AI Security Summit @RSAC

Safeguarding GenAI & Agentic Apps, Top 10 Risks in 2025

Moscone South, RM 308

Project Direction, Top 10 Risks for 2025, AI Security Landscape, Panels: Agentic Security, Red Teaming with AI open to **ALL RSAC Pass Levels**

2:00p-5:00pm

Agentic Security Open Workshop

Where? SPUR.org

654 Mission St, San Francisco

Registration Required

Join our project's Agentic Security Initiative workstream leaders for a deeper dive and collaborative discussion. **Open to All**

5:30p-8:30pm

Gen AI Security Community Networking Event

Where? SPUR.org

654 Mission St, San Francisco

Registration Required

A community event, network with project leaders, expert contributors, and peers

RSAC 2025 Conference